UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	**Cause No. 4:18CR00876JAR/NCC**
v.	)	
	)	
ASHU JOSHI,	)	
	)	
Defendant.	)	

MOTION TO SUPPRESS EVIDENCE & MEMORANDUM OF LAW

Comes now, Defendant, Dr. Ashu Joshi, by and through counsel, and moves this Court for an order suppressing all evidence seized or obtained from the illegal search of Defendant's confidential Facebook messages and photos, including but not limited to, Defendant's subsequent statement and consent to search his residence which was the fruit of an illegal search, and any evidence seized pursuant to any search warrant obtained using the illegally obtained information.

Specifically, Defendant was subject to an unlawful search and seizure made by Facebook and the National Center for Missing and Exploited Children. These unlawful searches violated Defendant's rights under the Fourth Amendment of the United States Constitution. Therefore, any evidence obtained from that search or subsequent investigation should be suppressed. This motion is made pursuant to the Fourth Amendment of the U.S. Constitution and Federal Rules of Criminal Procedure 12(b)(3) and 41. In support of this motion, Defendant submits the following:

FACTUAL BACKGROUND

1. Defendant, Dr. Ashu Joshi (hereinafter "Dr. Joshi"), has been charged by Indictment with Count I, Production of Child Pornography, in violation of 18 U.S.C. § 2251(a); Count

II, Transportation of a Minor Across State Lines, in violation of 18 U.S.C. § 2423(a) and 2; and Count III, Receipt of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(2).

2. On August 09, 2018, Jason Berry, a Trust & Safety Manger for social media website Facebook, was reviewing private messages exchanged between the Dr. Joshi and another Facebook user, M.D., obtained via a surveillance algorithm. Mr. Berry conducted independent research into the identity of the Facebook profiles he was surveilling and learned that one profile belonged to Dr. Joshi, and the other to M.D. a sixteen-year-old female.

3. On June 23, 2018 Dr. Joshi and M.D. were married in a private religious ceremony in the Commonwealth of Kentucky. This marriage was later recognized and validated by the Commonwealth of Kentucky on November 08, 2019, when a judge in the 27th Judicial Circuit of the Commonwealth of Kentucky, Knox County, signed an order recognizing the prior religious ceremony.[1]

4. Specifically, the Circuit Court Judge found and ordered that "the marriage conducted on June 23, 2018 between the parties is a valid marriage" and "that *as of* June 23, 2018 the parties are deemed married". *Id*. (emphasis added). *Id*. Dr. Joshi and M.D. have a child together as a result of their union.

5. The investigation against Dr. Joshi originated on August 09, 2018 when Jason Berry, a Trust & Safety Manger for social media website Facebook, was reviewing private messages exchanged between the Dr. Joshi and M.D., his wife, obtained via a surveillance algorithm. Mr. Berry conducted independent research into the identity of the Facebook profiles he was surveilling and learned that one profile belonged to Dr. Joshi, and the other to M.D.

[1] The marriage Order was attached an exhibit to Defendant's Motion to Dismiss which was also filed contemporaneously with this motion.

6. Between August 09, 2018, and September 30, 2018, Mr. Berry continued to monitor communications between the married couple. During that time Mr. Berry claims he observed 333 pictures and one video file being uploaded by M.D. to Dr. Joshi's private Facebook account. The pictures and video were of a private nature and contain sexual content. Some of the images were accompanied with private messages between M.D. and Dr. Joshi. Over this same period, Mr. Berry also claims he observed 144 images being uploaded from Dr. Joshi to M.D. One of the images contains a "still" from video chat between M.D. and Dr. Joshi.

7. None of the pictures or video were publicly shared or accessible to other users.

8. Despite observing this activity, Facebook did not suspend or terminate Dr. Joshi's account.

9. On October 5-6, 2018, Mr. Berry forwarded the results of his surveillance to the National Center for Missing & Exploited Children (NCMEC). NCMEC is a private non-profit organization which is obligated under federal statute to maintain a "tip line", and a duty to investigate and inspect suspected child pornography. 18 U.S.C. § 2258A and 42 U.S.C. § 5773(b). When an electronic service provider (ESP) gives information about suspected child pornography activity to NCMEC it is known as a "cyber tip". Cyber tips are generally forwarded on by NCMEC to law enforcement. NCMEC generated four Cyber Tips related to Mr. Berry's investigation, #41196177, #41222737, #41246874, and #41249019.

10. Once NCMEC received the flagged files and conversations, Courtney Holmes, a NCMEC analyst, took the file and opened it and reviewed its contents. Ms. Holmes utilized software to determine the "geo-location" of the IP address so that it could assist law enforcement in identifying the suspect. The geo-location for Dr. Joshi was determined to be in the Eastern District of Missouri,

while M.D.'s IP address was in Bowling Green, Kentucky. Ms. Holmes also conducted an extensive investigation into the identity of Dr. Joshi, including obtaining information on his medical license, employment history, residential history, telephone usage, and social media usage.

11. After obtaining this information, Ms. Holmes forwarded the Cyber Tips onto the Missouri Internet Crimes Against Children Taskforce, and the Kentucky State Police. Investigators with the St. Louis County Police Department reviewed the Cyber Tips and the contents of those tips.

12. At no time did Facebook, NCMEC, or local investigators seek out a search warrant, Grand Jury subpoena, or investigative subpoena to view the contents of those communications that comprise the Cyber Tips.

13. On October 10, 2018, investigators with the St. Louis County Police Department, using the information obtained from this warrantless surveillance, interviewed Dr. Joshi. During the interview Dr. Joshi admitted to conversing with M.D. about sexual subject matter and receiving and sending her pornographic material. Investigators also obtained Dr. Joshi's "consent" to seizure his electronic devices and cellular telephone. The consent was later revoked.

14. On October 16, 2018, Special Agent David Rapp of the Federal Bureau of Investigation, working in conjunction with the St. Louis County Police Department, obtained a search warrant for Dr. Joshi and M.D.'s Facebook account information. The search warrant requested the entire contents of the Facebook profiles, including (but not limited to) identifiers, activity logs, posts, group membership, "friends" lists, "check in" information, IP logs, search history, and all private messages and call history.

15. On December 18, 2018, Special Agent Rapp applied for and obtained a search warrant for the computers, cellphone, and other electronic devices taken from Dr. Joshi and Dr. Joshi's residence. Information obtained from those searches will be utilized against Dr. Joshi at trial.

LEGAL AUTHORITY & ARGUMENT

16. Evidence and statements obtained by investigators which the Government intends to use against Dr. Joshi were obtained pursuant to an unlawful search and seizure by Facebook, NCMEC, and the St. Louis County Police Department. Therefore, the search and seizure of this material is in violation of Dr. Joshi's Fourth Amendment protections guaranteed to him by the United States Constitution, and any and all "fruits" of that illegal search and seizure should be suppressed.

17. The Fourth Amendment provides that:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

U.S. Const. amend. IV. "The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz v. United States*, 389 U.S. 347, 351 (1967). "But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.*

18. The initial search of the conversations and images from Dr. Joshi's Facebook account was not conducted pursuant to a search warrant, Grand Jury subpoena, or investigative subpoena, and was not justified by valid consent or other lawful justification.

19. The Supreme Court has created an "exclusionary prohibition" for "evidence seized during an unlawful search". *See Wong Sun v. United States*, 371 U.S. 471, 484 (1963). That

exclusionary rule extends to "the indirect and the direct products of" an unlawful search because the indirect evidence constitutes "fruit" of the initial illegal action. *Id*. at 484-85. Therefore, the subsequent searches and seizures of Dr. Joshi's electronic equipment and other media contained therein, constituted illegal searches under the Fourth Amendment and violated Dr. Joshi's Constitutional privacy rights. Additionally, Dr. Joshi's statements to law enforcement must also be suppressed as fruit of this illegal search.

I. Dr. Joshi had a reasonable expectation of privacy in his private messages and photos on Facebook.

20. "[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). In determining whether an individual has a legitimate expectation of privacy, courts consider: (1) whether the individual, by his conduct has subjectively exhibited an actual subjective expectation of privacy; and (2) whether that subjective expectation is "one that society is prepared to recognize as 'reasonable.'" *Kyllo*, 533 U.S. at 33. Electronic communication, such as emails, have been held to enjoy Fourth Amendment protections. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

21. In the past, the question of whether one had a reasonable expectation of privacy to electronic content was, in part, dependent on the third-party doctrine. The third-party doctrine created with *United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979), essentially held that information shared with, or through, third parties had no reasonable expectation of privacy. However, since 2012 the Supreme Court has begun to move away from this approach with *United States v. Jones*, 565 U.S. 400 (2012), *Riley v. California*, 573 U.S. 373

(2014), and *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *See* Michael Price, *Rethinking Privacy: Fourth Amendment 'Papers' and the Third-Party Doctrine*, 8 J. Nat'l Security L. & Pol'y 247 (2016).

22. In *Jones*, the law enforcement "installed a GPS tracking device on the undercarriage of the [defendant's] Jeep while it was parked in a public parking lot." *Jones*, 565 U.S. at 403. "Over the next 28 days, the Government used the device to track the vehicle's movements, and once had to replace the device's battery when the vehicle was parked in a different public lot in Maryland." *Id.* "By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet and communicated that location by cellular phone to a government computer." *Id.*

While the holding of four Justices in *Jones* rested on a trespassory theory of the Fourth Amendment, the Supreme Court has repeatedly affirmed that the Fourth Amendment is not only concerned with trespassory intrusions on physical property, as the *Jones* Court itself recognized. "In *Katz*, [the] Court enlarged its then-prevailing focus on property rights by announcing that the reach of the Fourth Amendment does not 'turn upon the presence or absence of a physical intrusion.'" *Jones*, 565 U.S. at 414 (citing *Katz*, 389 U.S. at 353). Instead, *Katz* distinguished between what an individual has "knowingly expose[d] to the public" and "what he seeks to preserve as private, even in an area accessible to the public," when determining whether the Fourth Amendment's protections apply. *Katz*, 389 U.S. at 353.

In Justice Sotomayor's *Jones* concurrence, she noted that she would "take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements." *Id.* at 416 (Sotomayor, J.,

concurring). Justice Sotomayor also wrote that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Id. at 417. "This approach," she wrote, "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Id.*

23. In *Riley*, the Supreme Court once again recognized the principal that old rules governing searches and seizures in the context of physical objects do not make sense when applied to vast stores of digital data. 573 U.S. at 391. The Supreme Court held that "historical location information is a standard feature on many smartphones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." 573 U.S. at 390.

24. The most significant change the Supreme Court has made was last year with *Carpenter*. In *Carpenter*, the Court held that a warrant is required to access more than six days of historical "cell site location information" (CSLI), data obtained from the cellphone service provider indicating where a phone is connected to the cellular network. 138 S. Ct. at 2217. Writing for the Supreme Court, Chief Justice Roberts declined to "mechanically" apply the third-party doctrine. 138 S. Ct. at 2210. Instead, Chief Justice Roberts created a new doctrine which states courts should consider "the nature of the particular documents sought" to determine whether there is a legitimate expectation of privacy concerning their contents. 138 S. Ct. at 2212. This was a big doctrinal shift away from how many courts have understood and applied the third-party doctrine.

Relying on the two concurrences in *Jones*, the Court found that the CSLI data sought was intensely private information because it "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations". 138 S. Ct. at 2217. The data was found to be the "privacies of life" and presented an even greater concern than *Jones* or *Riley* because the cellphone is "almost a feature of human anatomy". 138 S. Ct. at 2214. CSLI data allows the government to "travel back in time to retrace a person's whereabouts," giving the police "access to a category of information otherwise unknowable". 138 S. Ct. at 2218.

The Court in *Carpenter* also shared a concern about any data that is created without an affirmative act by virtually any activity, and there is no way of avoiding leaving behind a trail. 138 S. Ct. at 2220. The Court stated that the user does not "assume the risk" of turning over this information because it is created without any affirmative act on their part. 138 S. Ct. at 2220.

25. In this case, Dr. Joshi had the requisite actual and subjective belief that the communications and content sent privately between he and his wife would be private. Dr. Joshi's subjective expectation of privacy in these electronic communications and content is one that society recognizes as reasonable.

26. The Electronic Communications Privacy Act ("ECPA") "protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers." 18 U.S.C. § 2510-22. "The Act applies to email, telephone conversations, and data stored electronically." *Id.* Both ECPA and the Stored Communications Act, 18 U.S.C. §§ 2701-2712, require that law enforcement go through appropriate application and affidavit procedures before a judge can enter an ex parte order authorizing or approving

interception of wire, oral, or electronic communications or retrieval of stored electronic communications. *See* 18 U.S.C. § 2518(1)-(3). No such order was sought in this case before law enforcement intercepted and stored communications.

27. ECPA itself provides remedies for persons aggrieved by violations of the Act, and criminalizes violations of the Act, including violations related to electronic communications. *Id.* Although ECPA does not provide an independent exclusionary rule for electronic communications, the fact that Congress enacted ECPA and specifically provided protections (including criminal penalties) for electronic communications provides compelling evidence that Congress has recognized the legitimacy of a privacy interest in electronic communications. 18 U.S.C. §§ 2511, 2515. If ECPA creates a reasonable expectation of privacy in electronic communications and the contents of those communications, then the search of a defendant's private messages without a warrant violates an individual's right to privacy guaranteed by the Fourth Amendment.

28. Furthermore, Dr. Joshi's electronic communications here are akin to the type of data of concern in *Carpenter*. The content "provides an intimate window" into Dr. Joshi's life. *Carpenter*, 138 S. Ct. at 2217. Electronic communications shared privately enjoy a reasonable expectation, and search and seizure of those communications violates the Fourth Amendment.

29. Finally, the expectation of privacy is higher when it concerns private content between spouses. This expectation of privacy has been recognized by the Supreme Court in holdings that married couples are entitled to privacy in the conduct of their most intimate relations. *See generally Eisenstadt v. Baird*, 405 U.S. 438 (1972) ("If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion

into matters so fundamentally affecting a person as the decision whether to bear or beget a child"); *Skinner*, 315 U.S. at 541 ("Marriage and procreation are fundamental to the very existence and survival of the race").

30. Martial privilege predates the U.S. Constitution and Bill of Rights and is part of American jurisprudence. *See Trammel v. United States*, 445 U.S. 40, 43-33 (1980) (tracing the marital privilege back to 1628). The marital communications privilege applies to any "information privately disclosed between husband and wife in the confidence of the martial relationship." *United States v. Brock*, 724 F.3d 817, 820 (7th Cir. 2013). The "basis of the immunity given to communications between husband and wife is the protection of martial confidences, regarded as so essential to the preservation of the marriage relationship as to outweigh the disadvantages to the administration of justice which the privilege entails." *Wolfe v. United States*, 291 U.S. 7, 14 (1934).

31. There is a presumption that all martial communications are confidential. *Blau v. United States*, 340 U.S. 332, 333 (1951) (citing *Wolfe*, 291 U.S. at 40). Martial privilege is recognized by federal courts. *See* Fed. R. Evid. 501; *SEC v. Lavin*, 111 F.3d 921, 933 (D.C. Cir. 1997) (recognizing the existence of martial privilege).

32. Here the martial privilege rule demonstrates that Dr. Joshi had a reasonable expectation of privacy in any conversations or images shared between him and his wife. The martial privilege cannot be overcome by the private party doctrine.

33. Based on the Government's intrusion into the reasonable expectation of privacy shared between Dr. Joshi and his wife, the evidence should be suppressed.

II. Facebook's search and seizure of private conversations and images is done in conformity with statutory and regulatory directions that have the practical effect of making Facebook an instrument of law enforcement.

34. The Fourth Amendment protects against unreasonable searches and seizures by private individuals or entities acting as "instruments or agents" of the Government". *See Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 613-14 (1989); *Collidge v. New Hampshire*, 403 U.S. 443, 487 (1971); *United States v. Highbull*, 894 F.3d 955, 991-92 (8th Cir. 2018).

35. "Whether a private party should be deemed an agent or instrument of the government for Fourth Amendment purposes necessarily turns on the degree of the government's participation in the private party's activities, a question that can only be resolved in light of all the circumstances." *United States v. Wiest*, 596 F.3d 906, 910 (8th Cir. 2010) (quoting *Skinner*, 489 U.S. at 614). In evaluating agency in the Fourth Amendment context, the Eighth Circuit has focused on three relevant factors: "[1] whether the government had knowledge of and acquiesced in the intrusive conduct; [2] whether the citizen intended to assist law enforcement or instead acted to further his own purposes; and [3] whether the citizen acted at the government's request." *Id.*

36. A statutory or regulatory scheme that clearly compels a private actor to take specific steps that further an enforcement goal will turn a private entity into a law enforcement instrument for Fourth Amendment purposes. *Skinner*, 489 U.S. at 615-16. Even where the government has not explicitly compelled a private entity to perform a search, its "encouragement, endorsement, and participation" in a search may rise to a level that implicates the Fourth Amendment. *Skinner*, 489 U.S. at 615-16.

37. The *Wiest* factors support the conclusion that Facebook's was acting as an agent of the government when it was scanning the content of the Dr. Joshi's private messages and photos. Congress's regulatory entrance into the field of ESPs and electronic content generally has produced a result substantially identical to the drug testing regulatory scheme of the Federal Railroad Safety Act that was at issue in the Supreme Court's *Skinner* decision.

In *Skinner*, the Supreme Court looked at regulations enacted pursuant to 45 U.S.C. § 431, which, though not compelling drug testing on the part of a rail operator, made reporting drug test results to the Federal Railroad Administration (FRA) mandatory. *Id*. at 607-11. Noting the fact that the railroad regulations at issue (1) pre-empted state law, (2) gave the Government the right to receive the evidence collected voluntarily by the railroad, and (3) forced the railroad to remove the employee from the regulated part of their job if they refused the request to be tested, the Court found that the Government had encouraged and endorsed the testing sufficient to implicate the government action triggering Fourth Amendment protection. *Skinner*, 489 U.S. at 615-16.

38. *Skinner* thus stands for the proposition that rather than merely being aware of or acquiescing in the private conduct, when the Government actively encourages, facilitates, or otherwise participates in the private search or seizure, its participation triggers Fourth Amendment protections regardless of the private party's intentions. *Id*.

39. 18 U.S.C. § 2258A, entitled Reporting Requirements of Electronic Communication Service Providers and Remote Computing Service Providers", mandates that internet service providers and electronic service providers (such as Facebook) that discover evidence of child pornography must report the information by way of cyber tip to NCMEC. 18 U.S.C. § 2258(a)(2)(A) requires, in turn, that NCMEC forward the report to the appropriate law

enforcement agencies. In this case, like the FRA regulations at issue in *Skinner*, the child pornography reporting statutes do not make screening email traffic for CP mandatory, but they mandate reporting any known violations for the purpose of initiating criminal investigations.

40. Although the statute recites a lack of intent to require ESPs to monitor their users' content, it also sets forth fines of up to $300,000 per violation for ESPs that were found to have willfully failed to make a report. *See* 18 U.S.C. § 2258A(f), *compare* 18 U.S.C. § 2258A(e). Just like the regulations in *Skinner*, Congress has held out the threat of sanction for non- compliance - here substantial fines if an ISP or ESP is found to have failed to make a report - which would predictably motivate ISPs and ESPs to perform due diligence in the interception of email traffic and search for illicit content. With the path to search cleared as it is by Congress, an ESP would run a substantial, if not certain, risk of criminal sanction if it exhibited willful blindness to contraband on its network by failing to proactively search all email traffic for content to ferret out suspected child pornography.

41. Additionally, the Government, through NCMEC, also facilitates ESP's searches by providing them with the "hash values" or SHA1 values they are supposed to look for. A hash value and SHA1 value are essentially computer code that identifies a computer image as unique, like a fingerprint. *See* Hany Farid, *Reining in Online Abuses*, Technology and Innovation, Vol. 19, pp. 593-599 (2018). Over a decade ago researchers at Dartmouth College, in collaboration with NCMEC and Microsoft, developed an algorithm named "PhotoDNA" to help identify the hash values of known child pornography images. *Id.* Presumably this was done with the use of some federal grant monies. The purpose of PhotoDNA was to help ESPs be better able to search

for child pornography on their systems. *Id*. The obvious involvement with NCMEC was for NCMEC to develop tools to give to ESPs for use in their searches.

In 2010, Facebook deployed the NCMEC provided PhotoDNA to its entire network. *Id*. As of 2016, NCMEC has supplied a database of over 80,000 images to ESPs, including Facebook, and all major social media companies are participating. *Id*. This shows the heavy involvement NCMEC has in directing ESPs to search their networks for contraband.

In this case, the defense is researching whether PhotoDNA, or some similar program, was used to identify the conversations or images shared between Dr. Joshi and his wife. Presumably Facebook is not manually reading every message or viewing every photo or image on their service due to the millions of images and conversations that are upload through their servers every day. If Facebook utilized an algorithm, like PhotoDNA or some similar program to search text, and if that algorithm was provided by the government or with the use of federal grant monies then that is further evidence of governmental control over ESPs.

42. Finally, it is worth noting that the statutory provision also provides immunity to ISPs and ESPs for actions relating to the "performance of the reporting or preservation responsibilities" under the statue. 18 U.S.C. § 2258B(a) & (b). *See also* 47 U.S.C. § 230 (statute immunizes ESP providers for implementation of screening software to search for child pornography of child exploitation). This is another way in ensuring the ESPs compliance with the governmental directive to search for child pornography.

43. The statutory schemes of 18 U.S.C. § 2258A and 47 U.S.C. § 230 described above make it clear that the government is far more than merely aware of, or simply acquiescing in, Facebook's search of content. Rather, Congress' actions constitute a unitary program to deputize

the ESPs in its fight against pornography and seek their assistance in ferreting out the suspected content in ways that its own law enforcement agencies could not do. These statutory schemes preempt state law that might otherwise restrict an ESP's authority to assist the authorities which has the effect of removing all legal barriers to searching for child pornography.

44. Not surprisingly, the statutory scheme has devolved to the de jure participation of ESP's as government investigating instruments. Because Facebook's actions in surveilling content is intertwined with government law-enforcement affiliated NCMEC's own efforts, the government is an active participant in Facebook's search and seizure of content and thus the search of Dr. Joshi's electronic content is subject to Fourth Amendment protections. *See Skinner*, 489 U.S. at 615-16.

45. Thus, read in a commonsense fashion, the statutory scheme of § 2258A, despite its disclaimer that it should not be construed "to require an [ISP or ESP] to monitor any user, subscriber, or customer," 18 U.S.C. § 2258A(f), constitutes "affirmative encouragement," "coercing," "dominating," or "directing" Facebook's efforts. That coercion, and the unitary law-enforcement endeavor to search it, engenders the Fourth Amendment. *Skinner*, 489 U.S. at 614-15. Because the Fourth Amendment dictates that a search without a warrant is unreasonable, and none was obtained to search the content of the Dr. Joshi's Facebook content, the evidence contained in the cyber tip reports and any evidence derived from it must be suppressed.

46. The Eighth Circuit has looked at this issue and reached a different conclusion under the facts of a different case. In *United States v. Stevenson*, 727 F.3d 826, 829-30 (8th Cir. 2013), the Eighth Circuit distinguished the statutory scheme mandating content report in pornography cases from the *Skinner* regulatory scheme. To the *Stevenson* court, § 2258A & B did not have a

specific direction to monitor their users and only set up a reporting requirement if illegal materials were observed. *Stevenson*, 727 F.3d at 830. (finding that "[a] reporting requirement, standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network"); *Accord United States v. Cameron*, 699 F.3d 621, 637-38 (1st Cir. 2012); *United States v. Richardson*, 607 F.3d 357, 366-67 (4th Cir. 2010),

47. However, the *Stevenson* court failed to address the provision for fines within § 2258A(e) which serve to compel search and seizure of contraband images or the fact that the government through NCMEC provides ESPs with the tools to perform searches (like has values or PhotoDNA) both of which have the effect of deputizing ESPs. It is precisely the point of the financial penalties to ESP under the statute to make it unacceptable and unpalatable for ESPs not to search content, and the government (through their agents) have given them the tools to do so. This is government "coercing", "dominating", and "directing" the search.

48. It is worth noting that cases such as *Stevenson* were decided before *Carpenter*; therefore, given the changes in the Supreme Court's view on electronic data, this Court should find that Dr. Joshi had a reasonable expectation of privacy in his communications. Furthermore, this Court should distinguish *Stevenson* for the failure to consider the punitive nature of § 2258A(e), and find that § 2258A transforms private ESPs, like Facebook, into government actors. 138 S. Ct. 2206 (2018).

49. In sum, the government compels the search of electronic content by ESPs, and when ESPs search that content it acts as an instrument of the government to conduct a search that the government cannot do on its own. The results of that search cannot be utilized as evidence and must be suppressed.

III. The National Center for Missing and Exploited Children qualifies as a government entity to which the Fourth Amendment applies. Absent a valid search warrant, the search and seizure of Dr. Joshi's private conversations and files and subsequent search of his home and the computers within his residence constituted an illegal search.

50. The next question the Court must resolve is whether NCMEC qualifies as a government entity and is thus bound by the Fourth Amendment. To answer the question this Court need not look very far. In *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), the Tenth Circuit Court of Appeals held (in an opinion written by now U.S. Supreme Court Justice Neil Gorsuch) that NCMEC was in fact a government entity. The *Ackerman* court found that NCMEC's statutory authority under 18 U.S.C. § 2258A and 42 U.S.C. § 5773(b) which require it to maintain a tipline and investigate tips for suspected child pornography qualify the center as a government entity.[2] *Id.* Thus, the boundaries of the Fourth Amendment apply to any search conducted by NCMEC. *Id.*

51. The second relevant question under the *Ackerman* opinion is whether the NCMEC investigation exceeded the scope of the "search" Facebook Messenger performed. Under the Supreme Court's "private search doctrine", a government entity does not conduct a Fourth Amendment search when it merely repeats an investigation already conducted by a private party. *Ackerman*, 831 F.3d at 1305 (*citing United States v. Jacobsen*, 466 U.S. 109 (1984)). However, if the search exceeds the scope of the private party investigation and amounts to more than merely

[2] The *Ackerman* opinion lays out over the course of several pages the Tenth Circuit's detailed analysis of this question. For the purposes of this motion, Defense Counsel merely cites to the underlying holding that is relevant to the Court's determination in this matter.

repeating what was done by the private party, then it constitutes a search under the Fourth Amendment. *Id*.

52. In *Ackerman*, the court held that NCMEC's review of emails associated with the suspect in order to identify the suspect was an illegal search and extended beyond merely collecting and forwarding information onto the appropriate law enforcement organization for further investigation. *Ackerman*, 831 F.3d at 1309.

53. Here, NCMEC not only received the files in question, but it reviewed the files, obtained the IP address and it geolocated it to the region it belonged to. Most concerning, NCMEC took all it knew and proactively tried to identify the suspect, just as they did in *Ackerman*. They utilized numerous tools at their disposable to investigate the Dr. Joshi, going so far as to review all his confidential residence history, locating information on his cellular phone, and social media sites. NCMEC even investigated his employment history and medical licenses.

54. This further investigation exceeds the scope of what Facebook performed which was merely flagging the files for further review. As such, the private search doctrine is inapplicable. *See Ackerman*, 831 F.3d at 1305-06 (holding that NCMEC's mere opening of an email forwarded to it by AOL containing child pornography images and subsequent submission of the images to local law enforcement for further investigation constituted "further investigation" under the private search doctrine).

55. In *Walter v. United States*, 447 U.S. 649 (1980), the Supreme Court considered whether law enforcement, once lawfully in possession of evidence delivered to it by a private entity, could further impinge on a defendant's expectation of privacy by expanding the search without first obtaining a warrant. *Id*. at 651. In that case, employees of a private entity received

and opened a package mistakenly delivered to it and discovered individual boxes of film suggestive of sexually explicit conduct. *Id*. at 652. They opened the packages but were unable to determine the content of the film inside. *Id*. The employees then forwarded the film packages to the FBI, who viewed the films and determined they were obscene. *Id*.

The Supreme Court held that the FBI's viewing of the films, even though it had lawful possession of them, was illegal absent a warrant. *Id*. at 654-55. This was so because the owner's privacy interest in the contents was not extinguished despite the fact that the film had been provided to the FBI by a private, third-party entity. *Id*. at 657. The FBI's subsequent viewing of the content represented "a significant expansion of the search by [the] private party and therefore must be characterized as a separate search" that could only be supported by exigency or a search warrant. *Walter*, 447 U.S. at 657.

56. Even assuming Facebook's search of the defendant's private content was a private action on their part (rather than government-compelled search), *see supra,* NCMEC's opening and viewing of the suspected contraband significantly expanded Facebook's search. The cyber tips strongly suggest that NCMEC's procedure is for its staff to perform a confirmatory examination once it receives the automatically generated cyber tip from the ESP, an examination that necessitates opening and viewing the file for content. *Id*. Thus, even assuming arguendo that Facebook was performing a private function rather than government search when it surveilled the Dr. Joshi's content, NCMEC's affirmative viewing of the actual images and messages once it was forwarded to its staff is exactly the kind of expansion of the search prohibited by *Walter.*

As in *Walter*, the fact that NCMEC may have received the cyber tip and been in possession of the image lawfully is not dispositive. *Id*. at 658. As the government was required to secure a

warrant before viewing the films in the boxes lawfully provided to it in *Walter*, so too the government here should have obtained a warrant before permitting NCMEC personnel to open and view the images provided to it by Facebook, regardless of whether NCMEC was lawfully in possession of the file or not. *Id*. at 657.

57. Just as in *Walter,* a warrant should have been obtained before the NECMEC search was conducted. The government did not, and thus the evidence of the content of the images and messages must be suppressed.

IV. Good faith does not apply.

58. Under *United States v. Leon*, 468 U.S. 897 (1984), "the good-faith exception does not apply when the affidavit in support of the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable" and "the exception does not apply when a warrant is so facially deficient that the executing officer could not reasonably believe it was valid.".

59. The exclusionary rule applies to a warrant not supported by probable cause, despite "good faith", when (1) the issuing magistrate was misled by an affidavit containing false information or information the affiant would have known was false except for his reckless disregard for the truth; (2) the issuing magistrate wholly abandoned his judicial role; (3) the search warrant application was "so lacking in indicia of probable cause as to render official belief" in the existence of probable cause "entirely unreasonable"; and (4) when the warrant is so facially deficient that the executing officer could not reasonably believe it was valid. *Leon*, 468 U.S. at 923.

60. In *United States v. Keith*, 980 F.Supp.2d 33, 42 (D. Mass. 2013), the court stated: if the ESP had sent suspect files directly to law enforcement instead of the NCMEC's CyberTip Line, "it could not seriously be contended that the law enforcement agency could open and inspect the contents of the file without regard to the Fourth Amendment's warrant requirement." With NCMEC's cooperation and collaboration with the various law enforcement and government entities and agents it's impossible to see how they could possibly claim ignorance of the law concerning warrantless searches. Merely because they were never challenged for illegal actions until recently does not absolve them of their prior wrongdoing.

61. Indeed, as *Ackerman* states: "In the face of so much law and evidence suggesting NCMEC qualifies as a government entity", there is no doubt NCMEC remains a government entity. *Ackerman*, 831 F.3d at 1298-1301. *Ackerman* found that the defendant had a reasonable expectation of privacy in his emails and "that sort of rummaging through private papers or effects would seem pretty obviously a 'search.'" *Ackerman*, 831 F.3d at 1304-06. Given *Ackerman*, Law enforcement knew or should have known of the risks associated with NCMEC's conduct in this case, and reliance on that conduct.

62. The exclusion of the fruit of the poisoned tree of the unconstitutional NCMEC searches, would "further the purpose of the exclusionary rule." *Leon*, 468 U.S. at 918. This Court's "inquiry is confined to the objectively ascertainable question of whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization." *Leon*, 468 U.S. at 922, n.23. This Court must review "all of the circumstances", and assume that the executing agents had "a reasonable knowledge of what the law prohibits". *Id.* at 919, n.20. The exclusionary rule's "good faith" exception does not apply.

63. The warrant's overbroad nature also demonstrate that good faith does not apply. Here, the warrant seeks the entire contents of the Facebook profiles, including (but not limited to) identifiers, activity logs, posts, group membership, "friends" lists, "check in" information, IP logs, search history, and all private messages and call history. It is so overbroad it constitutes a "general rummaging" of Dr. Joshi's content. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). The officer who signed the affidavit, Special Agent Rapp, is also the same one who executed the search by serving it on Facebook. Special Agent Rapp intentionally did not limit the search into the necessary account information and was therefore fully aware that his search warrant amounted to a general rummaging. Therefore, he cannot claim good faith when he knew the warrant exceeded a proper scope.

64. The search warrant also did not disclose the fact that Dr. Joshi and M.D. could have been married, even though that information was known to investigators. There are more than 200 references between Dr. Joshi and M.D. about their marital status, such as him calling M.D. his wife, throughout their chat logs. Investigators did not reference this anywhere in the search warrant affidavit. Therefore, investigators cannot rely on good faith when they know that all information was not submitted to the judge to review.

V. Conclusion

65. Facebook, NCMEC, and local investigators violated Dr. Joshi's Fourth Amendment protections when they illegally searched the contents of his private communications with his wife. No exception to this warrantless search applies. Therefore, all evidence and statements obtained that flow from that illegal search and seizure must be suppressed.

66. To deny this motion is to deny Dr. Joshi of the protections afforded to him under the Fourth Amendment of the United States Constitution.

67. Defense Counsel has personally conferred with the Government about the issues raised in the motion. Counsel has a good faith belief the government will seek to introduce the above referenced evidence.

WHEREFORE, the Defendant respectfully requests that this Court grant enter an order suppressing all evidence seized or obtained from the illegal search of Defendant's confidential Facebook messages and photos, including but not limited to, Defendant's subsequent statement and consent to search his residence which was the fruit of an illegal search, and any evidence seized pursuant to any search warrant obtained using the illegally obtained information and grant any other relief the Court deems just and proper.

Respectfully Submitted:

FRANK, JUENGEL & RADEFELD,
ATTORNEYS AT LAW, P.C.

By */s/ Daniel A. Juengel*
DANIEL A. JUENGEL (#42784MO)
Attorneys for Defendant
7710 Carondelet Avenue, Suite 350
Clayton, Missouri 63105
(314) 725-7777

CERTIFICATE OF SERVICE

I hereby certify that on November 22, 2019, the foregoing was filed electronically with the Clerk of the Court to be served by operation of the Court's electronic filing system upon the following.

Colleen Lang
Robert Livergood
Asst. United States Attorneys
111 South Tenth Street, 20th Floor
St. Louis, Missouri, 63102

/s/ Daniel A. Juengel
DANIEL A. JUENGEL